REMARKS

Claims 1-7 and 10-16 are currently pending in the present application.

Rejection under 35 U.S.C. § 103

Claims 1-4 and 10-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Paltenghe et al.* (US 6,421,729) in view of *Pond et al.* (US 4,864,616) and *Schneier*, Applied Cryptography, 2nd ed., John Wiley & Sons, Inc. 1996. Applicants respectfully traverse such rejection.

Claim 1 (and similarly Claim 10) recites steps of "in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key," and "storing said encrypted cookie in a non-protected storage device within said data processing system," "in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key" and "sending said decrypted cookie to said browser program."

Thus, according to the claimed invention, a cookie generated by an application from a remote server is encrypted by a public key of a public-private key pair before the cookie is stored in a non-protected storage device. When the encrypted cookie is being requested by a browser program, the encrypted cookie is then decrypted by a private key of the public-private key pair before sending to the browser program. As such, a cookie can be securely stored in a non-protected storage device of a data processing system.

On page 3 of the Final Office Action, the Examiner states that "Paltenghe does not expressly disclose a) a protected storage device for storing a[sic] encryption key pair; b) means for utilizing public key to encrypt cookie before storing it to the hard disk; c) means for utilizing private key to decrypt cookie." Applicants agree. It is not surprising that *Paltenghe* does not disclose any encryption of cookies because *Paltenghe* was never concerned about the security of the cookies. In fact, *Paltenghe* simply stores cookies in the hard drive of a user's computer in

the form a plain text file (col. 6, line 60-62), which is indicative of *Paltenghe*'s motivation did not lie upon cookie security.

Under MPEP § 706.02(j), in order to establish a *prima facie* case of obviousness, three criteria must be met. First, there must be some suggestion or motivation to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Third, the prior art reference(s) must teach or suggest all the claimed limitations. In the present case, the Examiner has not provided any reason or motivation for combining the teachings of *Paltenghe*, *Pond* and *Schneier*, especially when there is an indication in *Paltenghe* that cookie security is not a concern.

In addition, even though *Pond* and *Schneier* are related to cryptography, neither *Pond* nor *Schneier* teaches or suggests the claimed steps of "encrypting said cookie with said public key" and "decrypting said encrypted cookie with said private key." Because the claimed invention includes novel features that are not taught or suggested by *Spies*, the § 103 rejection is believed to be overcome.

CONCLUSION

Claims 1-7 and 10-16 are currently pending in the present application. For the reasons stated above, Applicants believe that independent Claims 1 and 10 along with their respective dependent claims are in condition for allowance. The remaining prior art cited by the Examiner but not relied upon has been reviewed and is not believed to show or suggest the claimed invention.

No fee or extension of time is believed to be necessary; however, in the event that any fee or extension of time is required for the prosecution of this application, please charge it against Deposit Account No. **50-0563**.

Respectfully submitted,

Antony P. Ng
Registration No. 43,427
BRACEWELL & PATTERSON, LLP
P.O. Box 969
Austin, Texas 78767-0969
(512) 472-7800

ATTORNEY FOR APPLICANTS